Notations et rappels.

· *Dans tout le problème, on désignera par p un nombre premier.*

· *On désigne par* $\mathbf{N}$ *l'ensemble des entiers naturels, par* $\mathbf{Z}$ *l'anneau des entiers relatifs, par* $\mathbf{Q}$ *le corps des nombres rationnels, par* $\mathbf{R}$ *le corps des nombres réels et par* $\mathbf{R}^+$ *l'ensemble des nombres réels positifs ou nuls.*

· *Pour a et b deux entiers relatifs tels que $a \leqslant b$, on note $[\![a;b]\!]$ l'intervalle d'entiers relatifs constitué des éléments de l'ensemble $\{a, a+1, ..., b-1, b\}$.*

· *Si n et k sont deux entiers naturels tels que $n \geqslant k$, alors le coefficient binomial $\binom{n}{k}$ vaut $\frac{n!}{k!(n-k)!}$.*

· *Soient m et n deux entiers naturels non nuls. Si* $\mathbf{K}$ *un anneau ou un corps, on note $\mathcal{M}_{m,n}(\mathbf{K})$ l'ensemble des matrices de taille $m \times n$ à coefficients dans* $\mathbf{K}$ *; si* $\mathbf{A}$ *est un sous-anneau de* $\mathbf{K}$*, alors $\mathcal{M}_{m,n}(\mathbf{A})$ est un sous-ensemble de $\mathcal{M}_{m,n}(\mathbf{K})$.*

· *Si d désigne un entier naturel non nul et* $\mathbf{K}$ *un anneau ou un corps, on note $\mathcal{M}_d(\mathbf{K})$ l'ensemble des matrices carrées de taille $d \times d$ à coefficients dans* $\mathbf{K}$*.*

· *On notera M^T la transposée d'une matrice M.*

· *La matrice identité I_d de $\mathcal{M}_d(\mathbf{K})$ est la matrice diagonale constituée uniquement de 1 sur la diagonale.*

· *L'ensemble des matrices inversibles de $\mathcal{M}_d(\mathbf{K})$ est noté $GL_d(\mathbf{K})$.*

· *On note $\mathbf{Z}_{/n\mathbf{Z}}$, l'ensemble des classes d'équivalence pour la relation de congruence modulo n, sur lequel on définit les lois $+$ et $\cdot$ induites par l'addition et le produit des entiers ; on rappelle que $(\mathbf{Z}_{/n\mathbf{Z}}, +, \cdot)$ est un anneau commutatif et que si p est un nombre premier, alors l'anneau $(\mathbf{Z}_{/p\mathbf{Z}}, +, \cdot)$ est un corps.*

· *On rappelle que la fonction indicatrice d'Euler associe à un entier naturel n non nul l'entier $\varphi(n)$ qui est le nombre de générateurs du groupe $(\mathbf{Z}_{/n\mathbf{Z}}, +)$, c'est aussi le nombre d'entiers $k \in [\![1;n]\!]$ qui sont premiers avec n.*

· *Si r et s sont deux entiers naturels non nuls premiers entre eux, alors on a l'égalité $\varphi(r)\varphi(s) = \varphi(rs)$.*

· *La partie entière d'un nombre réel x est notée $\lfloor x \rfloor$.*

· *On rappelle que si $(\mathbf{A}, +, \cdot)$ est un anneau commutatif, alors l'ensemble des éléments inversibles de* $\mathbf{A}$ *sera noté $\mathbf{A}^*$ et $(\mathbf{A}^*, \cdot)$ est un groupe abélien.*

Objectifs du problème.

Après un questionnaire "vrai ou faux" et deux exercices préliminaires dans lesquels on redémontre des résultats classiques du programme du concours, le problème est une introduction aux nombres p-adiques.

· La partie I du problème définit la valuation p-adique et la valeur absolue p-adique.

· Au début de la partie II, on définit l'anneau des entiers p-adiques. Ensuite, on s'intéresse au corps des fractions associé et à sa topologie.

· La partie III peut être abordée en admettant les derniers résultats de la partie II.

· La partie IV est indépendante de la partie III.

Ces deux dernières parties sont applications des parties I et II. On s'y intéresse à la structure de l'ensemble des termes nuls d'une suite récurrente linéaire et on y introduit l'exponentielle et le logarithme p-adique pour montrer que, lorsque p est un nombre premier impair, le groupe $\left((\mathbf{Z}_{/p^n\mathbf{Z}})^*, \cdot\right)$ est cyclique.

Vrai-Faux

1. Les affirmations suivantes sont-elles vraies ou fausses ? On justifiera soigneusement les réponses.

(a) Affirmation : « Pour tout nombre premier p et pour tout entier naturel n non nul, l'anneau $\left(\mathbf{Z}_{/p^n\mathbf{Z}}, +, \cdot\right)$ est un corps. »

Tournez la page S.V.P.

(b) Affirmation : « Si p est un nombre premier impair, alors la classe de 2 engendre le groupe multiplicatif des éléments inversibles de l'anneau $\left(\mathbf{Z}_{/p^n\mathbf{Z}}, +, \cdot\right)$. »

(c) Affirmation : « Le groupe multiplicatif des éléments inversibles de l'anneau $\left(\mathbf{Z}_{/9\mathbf{Z}}, +, \cdot\right)$est cyclique. »

(d) Si a un entier relatif, alors on note $\overline{a}$ la classe de a dans $\mathbf{Z}_{/5\mathbf{Z}}$.
Étant donnés quatre entiers relatifs a, b, c et d, on note M la matrice de $\mathcal{M}_2(\mathbf{Z})$ définie par $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et on note $\overline{M}$ la matrice de $\mathcal{M}_2(\mathbf{Z}_{/5\mathbf{Z}})$ définie par $\overline{M} = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}$.
Affirmation : « Si $M \in GL_2(\mathbf{R})$, alors $\overline{M} \in GL_2(\mathbf{Z}_{/5\mathbf{Z}})$. »

(e) Soient K et L deux corps commutatifs.
Affirmation : « Un morphisme d'anneaux $\mu : K \to L$ est toujours injectif. »

Exercice 1

Soit p un nombre premier, on désigne par $\mathbf{K}$ le corps $\mathbf{Z}_{/p\mathbf{Z}}$.

2. Soit E un $\mathbf{K}$-espace vectoriel et soit k un entier strictement positif. Notons $(x_1, \ldots, x_{k+1})$ une famille constituées de $k+1$ vecteurs de E telle que la famille $(x_1, \ldots, x_k)$ est libre.
Montrer que la famille de vecteurs $(x_1, \ldots, x_{k+1})$ est libre si et seulement si le vecteur x_{k+1} n'est pas combinaison linéaire des vecteurs $x_1, \ldots, x_k$.

3. Soient n et k deux entiers strictement positifs vérifiant la relation $k \leqslant n$.
Montrer par récurrence que le nombre de familles libres constituées de k vecteurs de $\mathbf{K}^n$ vaut $(p^n - 1)(p^n - p) \cdots (p^n - p^{k-1})$.

4. Soit n un entier strictement positif. Déterminer le cardinal de $GL_n(\mathbf{K})$.

Exercice 2

5. Soit n un entier naturel. On note $\mathcal{D}_n$ l'ensemble des entiers naturels qui divisent n. On souhaite montrer que pour tout entier n strictement positif on a l'égalité $n = \sum_{d \in \mathcal{D}_n} \varphi(d)$.

On pose $f(n) = \sum_{d \in \mathcal{D}_n} \varphi(d)$.

(a) Soit p un nombre premier. Pour tout entier i, calculer $\varphi(p^i)$. En déduire la valeur $f(p^k)$ pour tout entier k strictement positif.

(b) Soient m_1 et m_2 deux entiers naturels premiers entre eux. Montrer que l'application P

$$P : \begin{array}{ccc} \mathcal{D}_{m_1} \times \mathcal{D}_{m_2} & \to & \mathcal{D}_{m_1 m_2} \\ (d_1, d_2) & \mapsto & d_1 d_2 \end{array}$$

est bien définie et qu'elle est bijective.

(c) En déduire que lorsque m_1 et m_2 sont deux entiers naturels premiers entre eux on a la relation $f(m_1)f(m_2) = f(m_1 m_2)$.

(d) Montrer que pour tout entier n strictement positif on a l'égalité $n = \sum_{d \in \mathcal{D}_n} \varphi(d)$.

6. Soit $(\mathbf{K}, +, \cdot)$ un corps de cardinal fini égal à $c+1$. On a $\mathbf{K}^* = \mathbf{K} \setminus \{0\}$ et on souhaite montrer que le groupe $(\mathbf{K}^*, \cdot)$ de cardinal c est cyclique.
Pour tout entier d de $\mathcal{D}_c$, on note $N(d)$ le nombre d'éléments de $(\mathbf{K}^*, \cdot)$ qui sont d'ordre d.

(a) Déterminer la valeur de $\sum_{d \in \mathcal{D}_c} N(d)$.

(b) Soit d un élément de $\mathcal{D}_c$.

i. On suppose qu'il existe un élément x d'ordre d dans $\mathbf{K}^*$ et on note H le sous-groupe de $(\mathbf{K}^*, \cdot)$ engendré par x. En introduisant un polynôme judicieux, montrer que tout élément d'ordre d de $\mathbf{K}^*$ est dans H.

ii. Montrer que pour tous les éléments d de $\mathcal{D}_c$ on l'inégalité $N(d) \leqslant \varphi(d)$.

(c) Montrer que pour tout entier d de $\mathcal{D}_c$ on a l'égalité $N(d) = \varphi(d)$. En déduire que $(\mathbf{K}^*, \cdot)$ est un groupe cyclique.

Les résultats des deux exercices préliminaires pourront être utilisés dans le problème.

Problème

Dans tout le problème p désigne un nombre premier.

I. Valuation et valeur absolue p-adiques

I.A Définition de la valuation

7. Soit n un entier relatif non nul. Montrer qu'il existe un unique entier k tel que p^k divise n et p^{k+1} ne divise pas n.

L'unique entier k ainsi défini est appelé valuation p-adique de n et on le note $v_p(n)$.

8. Soient a et b deux entiers relatifs non nuls. Montrer l'égalité $v_p(ab) = v_p(a) + v_p(b)$.

9. En déduire que, si a, b, c et d sont quatre entiers relatifs non nuls qui vérifient la relation $\frac{a}{b} = \frac{c}{d}$ alors on a l'égalité $v_p(a) - v_p(b) = v_p(c) - v_p(d)$.

Étant donné un nombre rationnel non nul r, si a et b sont deux entiers relatifs non nuls tels que $r = \frac{a}{b}$, alors l'entier $v_p(r) = v_p(a) - v_p(b)$ est appelé valuation p-adique de r.

10. Montrer que si r et s sont deux nombres rationnels non nuls, alors on a l'égalité

$$v_p(rs) = v_p(r) + v_p(s)$$

11. Montrer que si r et s sont deux nombres rationnels non nuls tels que $r \neq s$, alors on a l'inégalité

$$v_p(r - s) \geqslant \min\big(v_p(r), v_p(s)\big)$$

Par convention, on pose $v_p(0) = +\infty$. Ceci permet de définir une application $v_p : \mathbf{Q} \to \mathbf{Z} \cup \{+\infty\}$.

12. En prenant soin de préciser les inégalités et les règles de calcul dans $\mathbf{Z} \cup \{+\infty\}$, vérifier que les résultats des questions **10.** et **11.** restent valables lorsque r et s sont deux nombres rationnels.

I.B Étude de $v_p(n!)$

Soit n un entier naturel non nul.

13. Étant donné un entier naturel k, on note E_k l'ensemble des entiers $i \in [\![1;n]\!]$ tels que $v_p(i) \geqslant k$. Décrire les éléments de E_k puis déterminer le cardinal de E_k.

14. Pour un entier i fixé dans $[\![1;n]\!]$, déterminer le nombre d'entiers k tels que $i \in E_k$. En déduire la formule

$$v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

15. *Application :* En utilisant la formule de la question **14.**, déterminer le nombre de zéros à la fin de l'écriture décimale de 100!.

16. Montrer que pour tout entier n strictement positif on la majoration suivante

$$v_p(n!) \leqslant \frac{n}{p-1}$$

I.C Une caractérisation des puissances de 2

Soit n un entier naturel non nul, il se décompose de manière unique en une somme

$$n = \sum_{i=0}^{q} u_i 2^i$$

où $q \in \mathbf{N}$, $(u_0, \cdots, u_q) \in \{0;1\}^{q+1}$ et $u_q \neq 0$. On définit alors $s(n) = \sum_{i=0}^{q} u_i$.

17. Pour tout entier k strictement positif, montrer que l'on a la relation $v_2(k+1) = s(k) - s(k+1) + 1$.

18. En déduire une expression de $v_2(n!)$ en fonction de n et $s(n)$.

19. Si n est une puissance de 2, montrer que pour tout entier $k \in [\![1;n-1]\!]$ le coefficient binomial $\binom{n}{k}$ est pair.

20. Montrer que si pour tout entier $k \in [\![1;n-1]\!]$ le coefficient binomial $\binom{n}{k}$ est pair, alors n est une puissance 2.

I.D Valeur absolue p-adique

On définit l'application $|\cdot|_p : \mathbf{Q} \to \mathbf{R}^+$ *par* $|0|_p = 0$ *et pour tout nombre rationnel* x *non nul* $|x|_p = \dfrac{1}{p^{v_p(x)}}$. *Cette application est appelée valeur absolue p-adique.*

21. Montrer que pour tout couple (x, y) de nombres rationnels on a

$$|xy|_p = |x|_p |y|_p \quad , \quad |x-y|_p \leqslant \max\big(|x|_p, |y|_p\big) \quad \text{et} \quad |x+y|_p \leqslant |x|_p + |y|_p$$

22. Soit d_p l'application

$$d_p \ : \ \begin{array}{ccc} \mathbf{Q}^2 & \to & \mathbf{R}^+ \\ (x,y) & \mapsto & |x-y|_p \end{array}$$

Montrer que pour tout triplet (x, y, z) de nombres rationnels on a l'inégalité suivante

$$d_p(x,z) \leqslant \max\left(d_p(x,y), d_p(y,z)\right)$$

Montrer que d_p est une distance sur $\mathbf{Q}$.

23. Étudier la convergence de la suite $\left(p^n\right)_{n\geqslant 0}$ dans l'espace métrique $(\mathbf{Q}, d_p)$.

II : Les entiers p-adiques

II.A. Définition de $\mathbf{Z}_p$

On note $\mathbf{Z}_p$ l'ensemble des suites $\left(a_n\right)_{n\geqslant 0}$ d'entiers naturels qui vérifient

- ▷ pour tout entier naturel n on a $a_n \in [\![0; p^{n+1}-1]\!]$,
- ▷ pour tous les couples d'entiers naturels n et m tels que $m \geqslant n$ on a $a_m \equiv a_n [p^{n+1}]$.

24. Soit $\left(a_n\right)_{n\geqslant 0}$ une suite d'entiers naturels telle que pour tout $n \in \mathbf{N}$ on a $a_n \in [\![0; p^{n+1}-1]\!]$. Montrer que la suite $\left(a_n\right)_{n\geqslant 0}$ est dans $\mathbf{Z}_p$ si et seulement si

$$\forall n \in \mathbf{N}\ ,\ a_{n+1} \equiv a_n [p^{n+1}]$$

25. Soit $a = \left(a_n\right)_{n\geqslant 0}$ un élément de $\mathbf{Z}_p$. Étant donné un entier n fixé, on décompose a_{n+1} en la somme $a_{n+1} = \sum_{i=0}^{n+1} u_i p^i$ où les u_i sont des entiers compris entre 0 et $p-1$.

Montrer que a_n se décompose en la somme $\sum_{i=0}^{n} u_i p^i$.

À tout élément $\left(a_n\right)_{n\geqslant 0}$ de $\mathbf{Z}_p$ on associe une unique suite $\left(u_i\right)_{i\geqslant 0}$ d'éléments de $[\![0; p-1]\!]$ telle que pour tout entier n on a l'égalité $a_n = \sum_{i=0}^{n} u_i p^i$.

26. Soit $a = \left(a_n\right)_{n\geqslant 0}$ un élément de $\mathbf{Z}_p$ dont les termes ne sont pas tous nuls. Montrer qu'il existe un unique entier naturel k vérifiant les relations suivantes

- ▷ $v_p(a_n) = +\infty$ si $n < k$,
- ▷ $v_p(a_n) = k$ si $n \geqslant k$.

Cet entier k est noté $\tilde{v}_p(a)$. Par convention, on pose $\tilde{v}_p(0) = +\infty$ où 0 est la suite de $\mathbf{Z}_p$ dont tous les termes sont nuls.

27. Soit $x \in \mathbf{Z}$ et soit $a = \left(a_n\right)_{n\geqslant 0}$ la suite d'entiers telle que, pour tout entier n, le terme a_n est le reste de la division euclidienne de x par p^{n+1}. Montrer que la suite a est un élément de $\mathbf{Z}_p$.

Cette suite sera notée $\theta(x)$ et on notera θ l'application $\theta : \mathbf{Z} \to \mathbf{Z}_p$ ainsi définie.

28. Dans cette question uniquement, fixons $p = 5$. Déterminer les éléments $\theta(7)$ et $\theta(-7)$ de $\mathbf{Z}_5$.

29. Montrer que θ est une application injective.

 Tournez la page S.V.P.

30. Soit $\alpha = (\alpha_n)_{n\geqslant 0}$ la suite définie par $\alpha_n = \sum_{i=0}^{n} p^i$ pour tout entier positif n. Vérifier que la suite α est un élément de $\mathbf{Z}_p$. Montrer qu'il n'existe pas d'entier relatif x tel que $\theta(x) = \alpha$.

31. Vérifier que pour tout entier relatif x on a la relation $\tilde{v}_p(\theta(x)) = v_p(x)$.

Les deux questions précédentes montrent que θ est une application injective de $\mathbf{Z}$ dans $\mathbf{Z}_p$ et que l'application $\tilde{v}_p$ prolonge l'application v_p à tous les éléments de $\mathbf{Z}_p$ via cette injection. Dans la suite du problème, l'application $\tilde{v}_p$ sera notée v_p.

II.B. Structure d'anneau

32. Soient $a = (a_n)_{n\geqslant 0}$ et $b = (b_n)_{n\geqslant 0}$ deux éléments de $\mathbf{Z}_p$. Pour tout entier n on note c_n le reste de la division euclidienne de $a_n + b_n$ par p^{n+1}. Montrer que la suite $c = (c_n)_{n\geqslant 0}$ est un élément de $\mathbf{Z}_p$.

On note cette suite $a + b$ ce qui munit $\mathbf{Z}_p$ d'une loi de composition interne notée $+$.

33. Déterminer un élément neutre, que l'on notera 0, pour la loi $+$. Étant donné un élément $a = (a_n)_{n\geqslant 0}$ de $\mathbf{Z}_p$, expliciter un élément $b = (b_n)_{n\geqslant 0}$ de $\mathbf{Z}_p$ tel que $a + b = 0$.
Montrer que $(\mathbf{Z}_p, +)$ est un groupe commutatif.

34. Soient $a = (a_n)_{n\geqslant 0}$ et $b = (b_n)_{n\geqslant 0}$ deux éléments de $\mathbf{Z}_p$. Pour tout entier n on note d_n le reste de la division euclidienne de $a_n b_n$ par p^{n+1}.

On admet que la suite $d = (d_n)_{n\geqslant 0}$ ainsi définie est dans $\mathbf{Z}_p$, elle sera notée $d = a \cdot b$. On admet également que $\cdot$ est une loi de composition interne qui permet de munir $(\mathbf{Z}_p, +, \cdot)$ d'une structure d'anneau commutatif.

Déterminer l'élément neutre de la multiplication dans l'anneau $(\mathbf{Z}_p, +, \cdot)$.

35. Montrer que $(\mathbf{Z}_p, +, \cdot)$ est un anneau intègre.

36. Montrer que si $a = (a_n)_{n\geqslant 0}$ et $b = (b_n)_{n\geqslant 0}$ deux éléments non nuls de $\mathbf{Z}_p$, alors on a les relations

$$v_p(a \cdot b) = v_p(a) + v_p(b) \quad \text{et} \quad v_p(a - b) \geqslant \min\big(v_p(a), v_p(b)\big).$$

37. Montrer que l'application θ définie dans la question **27.** est un morphisme injectif d'anneaux de $\mathbf{Z}$ dans $\mathbf{Z}_p$.
À l'aide de ce morphisme injectif, on identifie $\mathbf{Z}$ au sous-anneau $\theta(\mathbf{Z})$ de l'anneau $\mathbf{Z}_p$.

38. Soit $a = (a_n)_{n\geqslant 0}$ un élément de $\mathbf{Z}_p$. Montrer que a inversible dans $\mathbf{Z}_p$ si et seulement si le terme a_0 est non nul.

39. Soit $a = (a_n)_{n\geqslant 0}$ un élément de $\mathbf{Z}_p$. Montrer qu'étant donné un entier k, on a $v_p(a) \geqslant k$ si et seulement si il existe une suite $b = (b_n)_{n\geqslant 0}$ de $\mathbf{Z}_p$ telle que $a = \theta(p^k) \cdot b$.

40. Déterminer les idéaux de $\mathbf{Z}_p$.

Soit $E = \mathbf{Z}_p \times (\mathbf{Z}_p \setminus \{0\})$ et $\mathcal{R}$ la relation d'équivalence définie sur E par

$$(a, b)\mathcal{R}(c, d) \text{ si } a \cdot d = b \cdot c$$

Le corps des fractions de l'anneau intègre $\mathbf{Z}_p$ est l'ensemble quotient, noté $\mathbf{Q}_p$, des classes d'équivalence notées $\overline{(a, b)}$ de couples d'éléments $\mathbf{Z}_p \times (\mathbf{Z}_p \setminus \{0\})$ pour la relation d'équivalence $\mathcal{R}$. Il est muni des lois de composition internes induites par celles définies sur $\mathbf{Z}_p$, c'est un corps commutatif. En associant à un élément a de $\mathbf{Z}_p$ la classe de $(a, 1)$ dans $\mathbf{Q}_p$, on identifie $\mathbf{Z}_p$ à un sous-anneau de $\mathbf{Q}_p$.

41. Montrer que l'application

$$\begin{array}{rccl} \Theta : & \mathbf{Q} & \to & \mathbf{Q}_p \\ & \dfrac{a}{b} & \mapsto & \Theta\left(\dfrac{a}{b}\right) = \overline{(\theta(a), \theta(b))} \end{array}$$

est bien définie. Montrer ensuite qu'il s'agit d'un morphisme injectif de corps.

À l'aide de ce morphisme, on identifie $\mathbf{Q}$ *au sous-corps* $\Theta(\mathbf{Q})$ *de* $\mathbf{Q}_p$.

42. Montrer que, pour $\big((a,b),(c,d)\big) \in E^2$ tels que $(a,b)\mathcal{R}(c,d)$, alors $v_p(a) - v_p(b) = v_p(c) - v_p(d)$.

Cette valeur commune est appelée valuation p-adique de la classe de (a,b) *dans* $\mathbf{Q}_p$. *On la note* $v_p\big((a,b)\big)$.

43. Soit $x \in \mathbf{Q}_p$. Montrer que $x \in \mathbf{Z}_p$ si et seulement si $v_p(x) \geqslant 0$.

On admet que la valuation p-adique sur $\mathbf{Q}_p$ *vérifie les propriétés de la valuation dans* $\mathbf{Z}$ *démontrées dans la partie I. Cela permet de définir, comme dans* **I.D**, *la valeur absolue p-adique et la distance p-adique noté* d_p *sur* $\mathbf{Q}_p$.
On se place désormais dans l'espace métrique $(\mathbf{Q}_p, d_p)$. *On admettra que les opérations algébriques sur les limites des suites dans cet espace sont valides.*

II.C. Topologie dans $\mathbf{Q}_p$

44. Soit $a = \left(a_n\right)_{n\geqslant 0}$ un élément de $\mathbf{Z}_p$. Comme dans la question **25.**, on lui associe une suite $u = \left(u_n\right)_{n\geqslant 0}$ qui est constituée d'entiers compris entre 0 et $p-1$, telle que, pour tout entier n, on a $a_n = \sum_{i=0}^{n} u_i p^i$.
Montrer que pour tout entier k supérieur ou égal à $n+1$ on a l'inégalité $v_p(a_k - a_{n+1}) \geqslant n+1$.
En déduire que la suite $\left(\theta(a_n)\right)_{n\geqslant 0}$ converge vers a dans $\mathbf{Z}_p$.

On écrira alors $a = \sum_{i=0}^{+\infty} u_i p^i$.

45. Montrer que $\theta(\mathbf{Z})$ est dense dans $\mathbf{Z}_p$.

46. Soit a un élément de $\mathbf{Z}_p$ que l'on écrit $a = \sum_{i=0}^{+\infty} u_i p^i$. Soit l un entier. Montrer que $v_p(a) \geqslant l$ si et seulement si, pour tout i de $[\![0; l-1]\!]$ on a $u_i = 0$.

47. Soit $\left(a^{(k)}\right)_{k\geqslant 0}$ une suite de Cauchy de $\mathbf{Z}_p$. D'après la question **44.** on a

$$\forall k \geqslant 0, a^{(k)} = \sum_{i=0}^{+\infty} u_i^{(k)} p^i$$

où les termes $u_i^{(k)}$ sont des entiers compris entre 0 et $p-1$.

(a) Montrer que pour tout entier positif i, la suite $\left(u_i^{(k)}\right)_{k\geqslant 0}$ est stationnaire.

(b) En déduire que la suite $\left(a^{(k)}\right)_{k\geqslant 0}$ converge dans $\mathbf{Z}_p$.

On vient de montrer que que $\mathbf{Z}_p$ *est complet et on admet que* $\mathbf{Q}_p$ *est complet.*

Tournez la page S.V.P.

48. Soit $(x_k)_{k\geqslant 0}$ une suite d'éléments de $\mathbf{Q}_p$.

Pour $n \in \mathbf{N}$, on pose $S_n = \sum_{k=0}^{n} x_k$.

Montrer que la suite $(S_n)_{n\geqslant 0}$ converge dans $\mathbf{Q}_p$ si et seulement si la suite réelle $\left(|x_k|_p\right)_{k\geqslant 0}$ converge vers 0 (c'est-à-dire si et seulement si la suite $(x_k)_{k\geqslant 0}$ converge vers 0 dans $\mathbf{Q}_p$).

Par conséquent, dans $\mathbf{Q}_p$, une série est convergente si et seulement si son terme général tend vers 0.

III : Termes nuls d'une suite récurrente linéaire

Soient d un entier naturel non nul et $a = (a_0, \dots, a_{d-1}) \in \mathbf{Z}^d$ tel que $a_0 \neq 0$.
On s'intéresse à l'ensemble $\mathcal{R}_a$ des suites $u = (u_n)_{n\geqslant 0}$ définies par $(u_0, \dots, u_{d-1}) \in \mathbf{Z}^d$ vérifiant la relation de récurrence

$$\forall n \in \mathbf{N},\ u_{n+d} = a_0 u_n + a_1 u_{n+1} + \cdots + a_{d-1} u_{n+d-1}$$

Pour $u \in \mathcal{R}_a$, on notera

$$Z(u) = \left\{n \in \mathbf{N} \ / u_n = 0\right\}.$$

Étant donnés une suite u de $\mathcal{R}_a$ et un entier positif n, on pose $U_n = \begin{pmatrix} u_n \\ u_{n+1} \\ \vdots \\ u_{n+d-1} \end{pmatrix}$.

49. Déterminer une matrice A de $\mathcal{M}_d(\mathbf{Z})$ (indépendante de u) telle que, pour tout entier positif n, on ait $U_n = A^n U_0$. En déduire qu'il existe $X \in \mathcal{M}_{d,1}(\mathbf{Z})$ tel que, pour $n \in \mathbf{N}$, $u_n = X^T A^n U_0$.

50. Montrer que la matrice A est inversible.

51. On note $\overline{A}$ la matrice de $\mathcal{M}_d(\mathbf{Z}/p\mathbf{Z})$ obtenue à partir de A en réduisant chacun de ses coefficients modulo p. Montrer que l'on peut choisir un nombre premier impair p tel que la matrice $\overline{A}$ soit dans $GL_d(\mathbf{Z}/p\mathbf{Z})$.

On fixe désormais un tel p jusqu'à la fin de la partie **III**.

52. En déduire qu'il existe un entier strictement positif k et une matrice B de $\mathcal{M}_d(\mathbf{Z})$ tels que $A^k = I_d + pB$.

53. Soit $(f_j)_{j\geqslant 0}$ une suite de fonctions de $\mathbf{Z}$ dans $\mathbf{Z}$. Montrer que, pour tout entier n et pour tout entier j, la suite $\left(p^j \dfrac{f_j(n)}{j!}\right)_{n\geqslant 0}$ appartient à $\mathbf{Z}_p$.

54. Montrer que, pour tout entier naturel n, la série $S(n) = \sum_j p^j \dfrac{f_j(n)}{j!}$ converge dans $\mathbf{Q}_p$, puis qu'elle converge dans $\mathbf{Z}_p$.

On admet que si $S(n)$ s'annule pour une infinité de valeurs de n, alors $S(n)$ est nulle sur tout entier n dans $\mathbf{N}$.

55. Soient un entier k et une matrice B de $\mathcal{M}_d(\mathbf{Z})$ tels que l'on ait $A^k = I_d + pB$. Montrer que, si u est une suite appartenant à $\mathcal{R}_a$ et r est un entier compris entre 0 et $k-1$, alors l'ensemble

$$Z_r(u) = \left\{n \in \mathbf{N} \ / \ u_{kn+r} = 0\right\}$$

est soit fini, soit égal à $\mathbf{N}$.

IV : Exponentielle p-adique et application

IV.A. Définition de l'exponentielle

56. Soit x un élément de $\mathbf{Q}_p$. Montrer que, si $v_p(x) > \dfrac{1}{p-1}$, alors la série $\sum_{n \geqslant 0} \dfrac{x^n}{n!}$ converge.

On note alors $e_p(x) = \sum_{n \geqslant 0} \dfrac{x^n}{n!}$ *sa somme qui est appelée exponentielle p-adique de x.*

57. Montrer que, si x et y sont deux éléments de $\mathbf{Q}_p$ tels que $v_p(x) > \dfrac{1}{p-1}$ et $v_p(y) > \dfrac{1}{p-1}$, alors $e_p(x+y)$ est défini et vérifie la relation $e_p(x+y) = e_p(x)e_p(y)$.

58. Soit t un élément de $\mathbf{Q}_p$ tel que $|t|_p < 1$. Montrer que la série $\sum_{n \geqslant 1} (-1)^{n+1} \dfrac{t^n}{n}$ converge. On note $l_p(1+t)$ sa somme.

On admet que, pour $(u, v) \in \mathbf{Q}_p^2$ *tel que* $|u|_p < 1$ *et* $|v|_p < 1$, *on a* $l_p\big((1+u)(1+v)\big) = l_p(1+u) + l_p(1+v)$.
On admet également que lorsque ces quantités sont définies, on a $e_p\big(l_p(1+u)\big) = 1+u$ *et* $l_p\big(e_p(x)\big) = x$.

IV.B. Inversibles de $\mathbf{Z}/_{p^n}\mathbf{Z}$

Dans la suite, le nombre premier p sera impair et n sera un entier naturel supérieur ou égal à 2.
Pour $x \in \mathbf{Z}$, on notera $\overline{x}$ sa classe modulo p^n et $\tilde{x}$ sa classe modulo p. Soit H l'ensemble

$$H = \overline{1} + p\mathbf{Z}/_{p^n}\mathbf{Z} = \left\{\overline{1} + pu \ / \ u \in \mathbf{Z}/_{p^n}\mathbf{Z}\right\}.$$

59. Déterminer le cardinal de $\left(\mathbf{Z}/_{p^n}\mathbf{Z}\right)^*$.

60. Si $\cdot$ désigne le produit dans $\mathbf{Z}/_{p^n}\mathbf{Z}$, montrer que $(H, \cdot)$ est un sous-groupe de $\left((\mathbf{Z}/_{p^n}\mathbf{Z})^*, \cdot\right)$.

61. Soit π le morphisme surjectif de groupes de $\left((\mathbf{Z}/_{p^n}\mathbf{Z})^*, \cdot\right)$ dans $\left((\mathbf{Z}/_{p}\mathbf{Z})^*, \cdot\right)$ qui à $\overline{x}$ associe $\pi(\overline{x}) = \tilde{x}$.

(a) Montrer qu'il existe un entier relatif a tel que $\tilde{a}$ engendre le groupe $\left((\mathbf{Z}/_{p}\mathbf{Z})^*, \cdot\right)$ et tel que l'élément $\overline{a}$ soit d'ordre $p-1$ dans $\left((\mathbf{Z}/_{p^n}\mathbf{Z})^*, \cdot\right)$.

(b) En déduire qu'il existe un morphisme φ de groupes de $\left((\mathbf{Z}/_{p}\mathbf{Z})^*, \cdot\right)$ vers $\left((\mathbf{Z}/_{p^n}\mathbf{Z})^*, \cdot\right)$ tel que $\pi \circ \varphi$ soit l'identité de $(\mathbf{Z}/_{p^n}\mathbf{Z})^*$.

(c) Montrer que $\left((\mathbf{Z}/_{p^n}\mathbf{Z})^*, \cdot\right)$ est isomorphe au groupe produit $\left(\overline{1} + p\mathbf{Z}/_{p^n}\mathbf{Z}\right) \times \left(\mathbf{Z}/_{p}\mathbf{Z}\right)^*$ que l'on munit de la loi produit.

62. Montrer que si x est un élément de $p\mathbf{Z}_p$ alors $e_p(x)$ est un élément de $\mathbf{Z}_p$.

Tournez la page S.V.P.

63. Soit π_n le morphisme d'anneaux de $(\mathbf{Z}_p, +, \cdot)$ dans $(\mathbf{Z}_{/p^n\mathbf{Z}}, +, \cdot)$ suivant

$$\pi_n : \begin{array}{ccc} \mathbf{Z}_p & \to & \mathbf{Z}_{/p^n\mathbf{Z}} \\ \displaystyle\sum_{k=0}^{+\infty} u_k p^k & \mapsto & \displaystyle\sum_{k=0}^{n-1} \overline{u_k p^k} \end{array}$$

Où $\overline{x}$ désigne la classe d'un entier x dans $\mathbf{Z}_{/p^n\mathbf{Z}}$.

Soit $X \in p\mathbf{Z}_{/p^n\mathbf{Z}}$ qui est la classe de $x \in p\mathbf{N}$ (donc $x \in p\mathbf{Z}_p$). Montrer que $\pi_n\big(e_p(x)\big)$ ne dépend pas du représentant x choisi. On pose alors $E_p(X) = \pi_n\big(e_p(x)\big)$.

64. Montrer que $(p\mathbf{Z}_{/p^n\mathbf{Z}}, +)$ est isomorphe à $(\overline{1} + p\mathbf{Z}_{/p^n\mathbf{Z}}, \cdot)$.

65. *Application :* Utiliser ce qui précède pour déterminer un générateur de $\big(\overline{1} + 5\mathbf{Z}_{/125\mathbf{Z}}, \cdot\big)$.

66. Montrer que $\big((\mathbf{Z}_{/p^n\mathbf{Z}})^*, \cdot\big)$ est cyclique.

FIN DU SUJET